Opinion of the European Economic and Social Committee on 'Trust, privacy and security for consumers and businesses in the internet of Things (IoT)'

(own-initiative opinion)

(2018/C 440/02)

Rapporteur: **Carlos TRIAS PINTÓ**

Co-rapporteur: **Dimitris DIMITRIADIS**

Plenary Assembly decision	15/02/2018
Legal basis	Rule 29(2) of the Rules of Procedure
	Own-initiative opinion
Section responsible	Single Market, Production and Consumption
Adopted in section	04/09/2018
Adopted at plenary	19/09/2018
Plenary session No	537
Outcome of vote	182/3/2
(for/against/abstentions)	

1. **Conclusions and recommendations**

1.1. The internet of Things (IoT), thanks to its interconnectivity of persons and objects, offers a vast range of opportunities for individuals and businesses. These opportunities must be backed by a series of safeguards and controls so as to ensure introduction of the IoT is problem-free.

1.2. Since one of the pillars of the IoT is that decisions are taken automatically with no human input, it must be guaranteed that decisions do not undermine the rights of consumers or entail risks of an ethical nature or that are contrary to fundamental principles and human rights.

1.3. The EESC calls on the European institutions and EU Member States to:

1.3.1. ensure that security and privacy are protection by building appropriate regulatory frameworks that contain strict monitoring and control provisions;

1.3.2. clearly define the liability of all operators in the product supply chain and the related information flows, preventing legal loopholes occurring when several producers and distributors are involved at the same time;

1.3.3. introduce appropriate resources and effective coordination mechanisms between the European Commission and the Member States in order to guarantee consistent and harmonised application of both legislation subject to review and new rules, at the same time addressing the international scene;

1.3.4. monitor the development of emerging technologies associated with IoT, to guarantee high security, full transparency and fair accessibility;

1.3.5. promote European and international standardisation in order to guarantee product reliability, availability, resilience and continuation;

1.3.6. monitor the markets and protect a level playing field for the IoT's implementation, avoiding a concentration of transnational economic power with the new technology players;

1.3.7. undertake to promote awareness-raising and digital capacity-building initiatives reflecting basic research and innovation in the field;

1.3.8. guarantee the full implementation and effective use of alternative dispute resolution mechanisms both online and off-line (ADR and ODR);

1.3.9. encourage the existence, implementation and effective functioning of a European group action system that is able to put a stop to and obtain compensation also for situations where the use of the IoT causes damage or loss of a collective nature, as will be the case under the New Deal for Consumers.

1.4. Consumer confidence will result from strict compliance with the relevant legislation and the communication of best business practice concerning privacy and security, and the institutions are duty-bound to incorporate them into corporate social responsibility and socially responsible investment strategies.

1.5. The social and economic impact of the IoT will increase to the extent that it is sufficiently interlinked with the implementation of socio-environmental policies as part of the collaborative economy, the circular economy and the functional economy.

2. **Background and context**

2.1. The internet has burst onto the scene over the last 15 years, triggering transformations in every area of everyday life, impacting on various consumer habits. It is now forecast that over the next 10 years, the internet of Things (IoT) revolution will spread to the energy, farming and transport sectors, as well as to the more conventional sectors of the economy and society. This entails devising comprehensive policies that address this technological disruption with a smart approach.

2.2. The IoT concept first emerged from the Massachusetts Institute of Technology (MIT), basically meaning a world full of devices that are fully interconnected in such a way that the different interoperable processes can be jointly automated. The European Union has, for its part, been preparing to tackle digital convergence and the new challenges of the IoT, from the launch of 'i2010 — A European Information Society for growth and employment' plan ([1]), up to the recent IoT Action Plan (see Advancing the internet of Things in Europe, accompanying the 2016 Communication on Digitising European Industry — Reaping the full benefits of a Digital Single Market) ([2]).

2.3. The EESC has frequently discussed the fourth industrial revolution, marked by the convergence of digital, physical and biological technologies, and would draw particular attention to its 2017 opinion ([3]) on the subject. The IoT is effectively the ideal field for the most advanced forms of AI and is where the principles outlined by the EESC are put to the test, particularly the principle of the 'human in control'.

2.4. IoT devices often lack authentication standards which will keep user data safe. This results in the emergence of problems, since devices, data and supply chain partners are exposed to security breaches.

2.5. Emerging technologies like blockchain can solve security and trust issues: this can be used to track sensor data measurements and prevent not only duplication with any other malicious data but also safeguard the integrity and traceability of changes; a distributed ledger can provide IoT device identification, authentication and seamless secure data transfer; IoT sensors may be used for the exchange of data through a blockchain rather than a third party; device autonomy is enabled through the use of smart contracts, and also individual identity, integrity of data; creation and operation costs are reduced since there is no intermediary; finally, IoT devices on the blockchain provide a history of connected devices, which is valuable for any troubleshooting that may be required ([4]).

([1]) COM(2005) 229 final.
([2]) COM(2016) 180 final.
([3]) Artificial intelligence: The consequences of Artificial Intelligence on the (digital) single market, production, consumption, employment and society (OJ C 288, 31.8.2017, p. 1).
([4]) See Khwaja Shaik, *Why blockchain and IoT are best friends*, https://www.ibm.com/us-en/?lnk=m on the innovations in the European financial sector see OJ C 246, 28.7.2017, p. 8.

2.6. In contrast, open-code distributed ledger technologies are being developed for the exchange of information and value between IoT devices They do not allow data mining but use an architecture based on a mathematical concept known as a directed acyclic graph (DAG), avoiding commissions and ensuring that the network expands its capacity as the number of users increases.

2.7. In brief, we are faced with something that offers huge economic ([5]) and social potential, and great opportunities but also serious challenges associated with implicit risks, of a multi-disciplinary, cross-cutting nature that affects businesses and consumers, administrations and individuals equally. There should consequently be a shared approach to this issue but which at the same time recognises the specific character of different situations. It is worth mentioning United Nations estimates in this regard that by 2020 between 50 billion devices will be interconnected, providing consumer applications through televisions, refrigerators, security cameras, vehicles, etc.

2.8. IoT applications are already providing economic and social benefits as part of a globalised world, including services that are more responsive to the socioeconomic context, shorter feedback cycles, remote repairs, decision-making support, better allocation of resources and remote control of services. However, a number of related and highly sensitive factors arise, such as privacy and security, information asymmetry, the transparency of transactions, complex responsibilities, the blocking of products and systems and also the rise of hybrid products that can affect ownership, exposing consumers to the remote application of contracts, with the consequent weakening of guarantees.

2.9. The huge legal challenges faced by the EU and its Member States stem from the fact that many of the specific features of the IoT (high levels of complexity and interdependence, the element of autonomy, the components of data generation and/or processing, and an open dimension) are shared with other emerging digital technologies such as blockchains, 3D printing and cloud computing. In the EESC's view, the European Commission's Staff Working Document ([6]) on liability for emerging digital technologies is a further step in the right direction.

2.10. Ultimately, maximising the benefits and minimising the risks associated with the IoT means providing accessible, clear, concise and accurate information, promoting in particular digital inclusion and connectivity for more vulnerable consumers by designing fully traceable products and services that incorporate integrated trust, privacy and security standards.

3. **Consumer and business trust in the IoT**

3.1. The IoT is a complex ecosystem that enables devices from different manufacturers, distributors or software developers to be interconnected. This can lead to difficulties in identifying responsibility where regulations are breached or when third parties or systems suffer material loss or other damage caused by defective products or by products that are misused by third parties, excluding end-users, via the internet. It is indeed possible that many operators involved in the global product value chain are not sufficiently knowledgeable or experienced in terms of security or data protection for on-line devices.

3.2. A new focus on responsibilities is therefore needed, aimed at ensuring that both consumers and businesses adopting IoT applications are protected in an environment in which properly-configured products may become defective and unsafe as a result of digital security incidents or unauthorised misuse (such as hackers). This environment should make it possible to anticipate, prevent and protect against automated decisions that may erode universally recognised ethical principles and human rights.

([5]) Digital McKinsey estimates that the IoT possesses a potential economic impact of between USD 3,9 and 11,1 trillion annually.
([6]) SWD(2018) 137.

3.3. The EESC welcomes both the revision of the application of the 1985 Directive on liability for damage caused by defective products ([7]), together with the recent creation of the multistakeholder expert group on liability and new technologies, with a view to ensuring a fair balance between the interests of producers and of consumers. A new framework of responsibilities should make clear provision for the traceability of responsibility and safety at every stage of the product value chain and throughout its estimated lifecycle, incorporating sustainability as a new factor that will make product updating, improvement, portability, compatibility, reuse, repair or adjustment a requirement.

3.4. Where the IoT is concerned, specific consideration must also be given to identifying the liability of all operators in the product supply chain, preventing legal loopholes occurring when several producers and distributors are involved at the same time. The EESC considers it essential to clearly specify the procedures to be followed by consumers in each case, promoting alternative dispute resolution (ADR) mechanisms.

3.5. The EESC stresses the importance of pre-contractual information, transparent contract clauses and clear operating instructions for devices; possible associated risks and safeguards should be explicitly highlighted.

3.6. The interoperability and compatibility of devices and associated software must be ensured, in order to prevent problems and make it possible for the consumer to compare providers. The EESC stresses that this factor is also key to establishing a level playing field between large companies and SMEs.

3.7. Finally, the EESC advocates respect for net neutrality and urges the Commission to carry out strict monitoring of market behaviour.

4. **Consumer privacy in the IoT**

4.1. The ability of consumers to check their personal data and privacy preferences has been improved with the new General Data Protection Regulation (GDPR) ([8]). The user of a device must have control over how the data generated are to be used and who may have access to them, since the diversity of data, as well as their accumulation and links with other data, mean that there is a serious risk to privacy in the IoT ecosystem.

4.2. The effect that the multiplicity of products, services or entities may have on privacy and data protection, when data are transferred autonomously due to their interconnectivity, must not be overlooked. Similarly, in cases where information is processed or reformulated using initially harmless data, a clear picture of individuals' habits, locations, interests and preferences could be built up, making the user profile easier to access and trace.

4.3. Legal guarantees must ensure that users are fully able to exercise their rights to privacy and personal data protection without any restriction. This would avoid potential harm such as discriminatory practices, invasive advertising, loss of privacy and breaches of security. Consumers, for their part, must have information on the economic value of their data and reserve the right to share them.

4.4. As provided for in the GDPR, businesses and regulators must regularly review the scope of personal data collection and assess the extent to which processed data are proportionate and necessary to the provision of the service. The various aspects and impacts of privacy must be evaluated at every stage in the conception, design and development of any connected product and the online ecosystem in which it operates (privacy by design). Hence, the principles of privacy by design and privacy by default must be implemented consistently in the IoT.

4.5. All connected products must consequently be configured according to a pre-determined model based on the highest level of protection of privacy (by design and by default), preventing the unwanted tracing of user behaviour and occupations.

([7]) COM(2018) 246 final.
([8]) In force since 25 May 2018.

4.6. In any case, consumers must have reliable knowledge of the data compiled, who has access to them and the purpose to which they are to be put while the link to the product or service remains active, and also of the applicable privacy policy, and must know if the algorithms used affect quality, price or access to a service.

5. **Consumer and business security in the IoT**

5.1. The interconnectivity of devices that characterises the IoT ecosystem may foster the development of unlawful or undesirable technological practices, becoming a space in which vulnerability can flourish and propagate virally. There must therefore be a comprehensive approach to security covering each and every component of the system.

5.2. The supply of products and cybersecurity-related updates will have to be justified and provide cover not only for individual devices, but must also be extended to security risks arising from interconnectivity with other devices in the IoT: quality standards for security should not be watered down due to the number of such devices.

5.3. In this regard, the proposal for a Regulation on the EU Cybersecurity Agency ([9]) contains a certification framework for the information and communication technologies which will provide for voluntary safety certification and labelling for different types of products, including those on the IoT. While the EESC welcomes this measure, it also expresses concern that it is not compulsory.

5.4. Cybersecurity measures should cover risks arising from any kind of vulnerability, particularly hacking, unauthorised access or misuse and the risks surrounding payment methods and financial fraud. In this regard, the EESC agrees with the remit given to the multistakeholder expert group on liability and new technologies.

5.5. The safety and security of individual users must also be addressed given risks such as the use of proximity, shared bandwidth, exposure to electromagnetic fields and possible interference with connected life-sustaining devices. The EESC backs the application of supervisory and preventive product-withdrawal arrangements for risks to consumers' health and safety or to their private, economic interests.

5.6. Businesses must adopt standards aligned with best practice, such as security by design and by default, and accept external, independent evaluations. In the event of security incidents or data breaches, businesses will be obliged to report such incidents, including information on liability for damage and non-compliance with legislation.

5.7. Businesses must give consumers simple, accessible information that enables them to take appropriate decisions and to adopt safe practices, providing the necessary security updates throughout the lifecycle of the product.

5.8. The lack of consistent standards related to IoT networks must be addressed. Advanced broadband and new generation technologies must be implemented to improve current infrastructure.

6. **Proposals for action in the framework of public policy** ([10])

6.1. The public authorities, in exercising their powers in the various territories of the European Union, must actively engage in developing IoT policies and action plans with the aim of achieving a balance of interests of the various stakeholders, anticipating and guarding against possible adverse impacts. The EESC advocates:

6.1.1. creating sand boxes, i.e. physical spaces, clusters, etc., to run pilot projects and proofs of concept. These should aim not at testing just technologies, but also regulatory models ([11]);

([9]) See COM(2017) 477 final.
([10]) See World Bank Group, internet *of things: The New Government-to-Business Platform*.
([11]) See https://ec.europa.eu/digital-single-market/en/news/eu-and-eea-member-states-sign-cross-border-experiments-cooperative-connected-and-automated

6.1.2. financing technology infrastructure that allows the development of innovative IoT projects under the new Horizon Europe programme;

6.1.3. appointing independent institutes and agencies as facilitators and caretakers of IoT projects. The EESC welcomes the relevant measures set out in the 2017 Regulation on cybersecurity and calls on the Commission to effectively promote standardisation processes in the digital industry using appropriate budgetary resources ([12]);

6.1.4. promoting public-private cooperation platforms and partnerships, bringing in the scientific community, industry and consumers;

6.1.5. fostering investment in the development of local business models harnessing the benefits of the IoT and making it easier to tackle complex aspects such as data protection and ownership;

6.1.6. carrying out capacity-building in the business world with a view to co-responsibility. It should be ensured that security and privacy by design and by default are built into ITC products and services, in keeping with the principle of 'duty of care' advocated in the new Cybersecurity Regulation. In this connection, the EESC welcomes the planned drafting of **codes of conduct** to complement regulation;

6.1.7. encouraging European and international standardisation initiatives to ensure the essential characteristics of IoT systems, i.e. reliability, safety, availability, resilience, maintainability and use. In particular, standardisation is essential for the rapid realisation of highly digitised industrial manufacturing processes;

6.1.8. ensuring that IoT users, especially the most vulnerable or those living in sparsely populated areas, have affordable, high-quality access;

6.1.9. promoting awareness-raising campaigns and education programmes to facilitate adoption of the IoT by businesses and consumers, enabling them to acquire the necessary capacities and skills ([13]), paying particular attention to vulnerable groups and diversity;

6.1.10. launching initiatives in the educational sphere to ensure sufficient prevention, given young children's early entry into digital environments;

6.1.11. launching diagnostic analyses and studies of the impact of IoT on areas such as new models of sustainable production and consumption;

6.1.12. guaranteeing the full implementation and effective use of alternative dispute resolution mechanisms both online and off-line (ADR and ODR);

6.1.13. encourage the existence, implementation and effective functioning of a European group action system that is able to put a stop to and obtain compensation also for situations where the use of the IoT causes damage or loss of a collective nature, as will be the case under the New Deal for Consumers.

6.2. The EESC also calls on the Commission to evaluate the rules directly or indirectly related to the IoT and, where necessary, to improve the existing legislation. In this connection, the ***New Deal for Consumers*** should also focus on interconnected devices, networks and their security, and the data associated with such devices.

6.3. Finally, the EESC stresses the importance of establishing cooperation and coordination mechanisms between the Member States for the efficient and uniform application of the planned rules and for the agreements that the European Union must draw up beyond its borders due to the places of establishment of companies and suppliers, with particular emphasis on the exchange of best practice. International policy on cross-border data flows must be coordinated so that the countries involved can establish equally high standards of protection in their national law, both substantial and procedural.

Brussels, 19 September 2018.

The President
of the European Economic and Social Committee
Luca JAHIER

([12]) OJ C 197, 8.6.2018, p.17.
([13]) OJ C 434, 15.12.2017, p. 36.